



IN THE UNITED STATES PATENT & TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application of:
ATKINS ET AL.

Serial No.: **09/651,548**

Filed: **AUGUST 29, 2000**

Title: **SYSTEM, METHOD AND
PROGRAM FOR MANAGING A USER
KEY USED TO SIGN A MESSAGE
FOR A DATA PROCESSING SYSTEM**

Attorney Docket No.: **RPS920000026US1**

Examiner: **SHIN, KYUNG H.**

Group Art Unit: **2143**

APPEAL BRIEF UNDER 37 C.F.R. § 1.192

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is submitted in support of the appeal in the above-referenced application. Please charge the fee of **\$500.00** due under 37 C.F.R. §1.17(c) for filing the Brief to **Lenovo Inc. Deposit Account No. 50-3533**. Appellants respectfully request an extension of time within the first month and enclose a check for \$120.00. No additional fee is believed to be required; however, if additional fees are required, please charge **Lenovo Inc. Deposit Account**

No. 50-3533.

11/04/2005 DTESSEN1 00000118 503533 09651548

01 FC:1251
02 FC:1402

120.00 OP

500.00 DA

CERTIFICATE OF MAILING
37 C.F.R. § 1.8(a)

I hereby certify that this correspondence is being deposited with the United States Postal Service on the below listed date with sufficient postage for first-class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: 11/1/05

By: Vicki J. Lipson
Signature

REAL PARTY IN INTEREST

The real party in interest in the present Appeal is Lenovo Inc., the Assignee of the present application.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellants, the Appellants' legal representative, or assignee, which directly affect or would be directly affected by or have a bearing on the Board's decision in the pending Appeal.

STATUS OF CLAIMS

Claims 1-24 were originally presented. In Appellants' Amendment A, filed May 18, 2004, Claims 1, 3, 6-7, 9, 11, 14-15, 17, 19 and 23 were amended, and no claims were canceled or entered. No further amendments to the claims were proposed or entered. Claims 1-24, which comprise all pending claims, stand finally rejected by the Examiner as noted in the Office Action dated June 17, 2005. The rejection of Claims 1-24 is appealed.

STATUS OF AMENDMENTS

Appellants' Amendment A, filed May 18, 2004, was entered by the Examiner. No amendments to the claims have been proposed or entered subsequent to the final rejection that led to this appeal.

SUMMARY OF THE CLAIMED INVENTIONS

The invention recited in independent Claim 1 provides a method for managing a user key used to sign an electronic message. As depicted in step 304 of Figure 3 and described at page 14, lines 1-4, the method includes assigning a user key to a user and storing the user key in an encrypting data processing system utilized to encrypt messages. The encrypting data processing system can then encrypt messages with the user key, as depicted in step 306 of Figure 3 and as described at page 14, lines 7-9. According to the claimed method, an associated key is also stored in the encrypting data processing system and used to encrypt to obtain an encrypted user key, as illustrated at step 310 of Figure 3 and as described at page 14, lines 25-27. The encrypting data processing system communicates at least one encrypted message together with the encrypted user key to a recipient system in order to permit validation of an association of the

user with the encrypted messages by the recipient system, as shown at step 318 of Figure 3 and described at page 15, lines 4-15. Thereafter, validation of the association of the user with messages can be prevented by revoking the associated key at the encrypting data processing system, as depicted at block 320 of Figure 3 and as described at page 15, lines 17-33.

The invention recited in independent Claim 9 provides a system for managing a user key used to sign an electronic message. Each of the elements of the system recited in Claim 9 is set forth in the means-plus-function format permitted by 35 U.S.C. § 112, paragraph 6. An exemplary data processing system 100 embodying the claimed system includes means for assigning a user key to a user (e.g., server system 104 of Figure 1), which assigns a user key to a user as depicted in step 304 of Figure 3 and described at page 14, lines 1-4. Data processing system 100 further includes means for storing a user key 103a, 103b, 103c, such as hard disks 19, 29 of Figure 2. Data processing system 100 also includes means for encrypting the messages with the user key (e.g., encryption chip 106), as depicted in step 306 of Figure 3 and as described at page 14, lines 7-9. As depicted at reference numeral 120 of Figure 1, data processing system 100 also includes protected storage that serves as a means for storing an associated key (e.g., key A, key B, key C). Encryption chip 106 of data processing system 100 of Figure 1 further serves as a means for encrypting the user key with the associated key to obtain an encrypted user key, as illustrated at step 310 of Figure 3 and as described at page 14, lines 25-27. Data processing system 100 also includes means for communicating at least one encrypted message together with the encrypted user key to a recipient system (e.g., LAN interface 16 of Figure 2) in order to permit validation of an association of the user with the encrypted messages by the recipient system, as shown at step 318 of Figure 3 and described at page 15, lines 4-15. Data processing system 100 further includes means (e.g., encryption chip 106) for thereafter preventing validation of the association of the user with messages by revoking the associated key in said system, as depicted at block 320 of Figure 3 and as described at page 15, lines 17-33.

Dependent Claim 15 recites in the means-plus-function format provided for in 35 U.S.C. § 112, paragraph 6, a system for managing a user key used to sign an electronic message. Claim 15, which depends on Claim 13, recites, in addition to the features of Claim 13, means (e.g., client system 102 and its LAN interface 16) for communicating an encrypted associated key to

validate the association of the user with the encrypted messages, as described at page 15, lines 4-15 and depicted in Figure 3 at block 318.

The invention recited in independent Claim 17 provides a program product for managing a user key used to sign a message. The program product includes a control program (method 300 of Figure 3; page 13, lines 15-19) and a computer usable media bearing the control program (e.g., hard disks 19, 29 of Figure 2). Each of the elements of the control program recited in Claim 17 is set forth in the means-plus-function format permitted by 35 U.S.C. § 112, paragraph 6. These elements include instruction means for assigning a user key to a user and for storing the user key in an encrypting data processing system utilized to encrypt messages, as depicted in step 304 of Figure 3 and described at page 14, lines 1-4; instruction means for encrypting the messages with the user key, as depicted in step 306 of Figure 3 and as described at page 14, lines 7-9; instruction means for storing an associated key in the encrypting data processing system and for encrypting the user key with the associated key to obtain an encrypted user key, as illustrated at step 310 of Figure 3 and as described at page 14, lines 25-27; instruction means for communicating at least one encrypted message together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system, as shown at step 318 of Figure 3 and described at page 15, lines 4-15; and instruction means for thereafter preventing validation of the association of the user with messages by revoking the associated key within the encrypting data processing system, as depicted at block 320 of Figure 3 and as described at page 15, lines 17-33.

Dependent Claim 23 recites in the means-plus-function format provided for in 35 U.S.C. § 112, paragraph 6, a program product for managing a user key used to sign an electronic message. Claim 23, which depends on Claim 17, recites, in addition to the features of Claim 17, instruction means (e.g., method 300 of Figure 3; page 13, lines 15-19) for communicating an encrypted associated key to validate the association of the user with the encrypted messages, as described at page 15, lines 4-15 and depicted in Figure 3 at block 318.

GROUND OF REJECTION

The present Appeal is filed in response to the Final Office Action dated June 17, 2005, and labeled Paper No. 20050612, in which the following rejections are made:

(1) Claims 1-3, 6-11, 14-19, and 22-24 are rejected under 35 U.S.C. § 103 as unpatentable over U.S. Patent No. 6,807,277 to *Doonan et al.* (*Doonan*) in view of U.S. Patent No. 6,009,177 to *Sudia*;

(2) Claims 4, 12 and 20 are rejected under 35 U.S.C. § 103 as unpatentable over *Doonan* and *Sudia* in view of U.S. Patent No. 6,732,101 to *Cook*; and

(3) Claims 5, 13 and 21 are rejected under 35 U.S.C. § 103 as unpatentable over *Doonan* and *Sudia* in view of U.S. Patent No. 4,888,800 to *Marshall*.

ARGUMENT

I. The combination of *Doonan* and *Sudia* does not disclose each claimed feature of exemplary Claim 1

Appellants respectfully submit that the combination of *Doonan* and *Sudia* does not render exemplary Claim 1 (and similar Claims 9 and 17) of the present invention unpatentable under 35 U.S.C. § 103 because the combination of cited references does not disclose each feature recited therein. For example, the combination of *Doonan* and *Sudia* does not disclose the following steps of exemplary Claim 1:

storing an associated key in the encrypting data processing system and encrypting the user key with the associated key to obtain an encrypted user key;

...

thereafter, preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system.

With respect to the claimed “associated key”, page 3 of the present Office Action cites col. 5, lines 63-67 of *Doonan*, which disclose:

The composite message P is first encrypted to form encrypted message Pe, using a randomly-generated symmetric encryption key Ks. The symmetric key Ks is then itself encrypted using the public key published in a digital certificate owned by the recipient, to form [the encrypted symmetric key] Kp. (emphasis supplied)

Thus, *Doonan's* public key of the message recipient is relied upon in the present rejection as disclosing the claimed “associated key.” Under this mapping of claim elements, obviousness is only established if the combination of cited references disclose (in the words of Claim 1), “preventing validation of the association of the user with messages by revoking” the public key of the message recipient at the encrypting data processing system.

With reference to the step of “preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system”, page 4 of the present Office Action correctly notes that *Doonan* does not disclose revocation of an associated key as claimed. However, the Office Action then relies upon *Sudia's* disclosure at col. 22, lines 51-63 of the conventional revocation of a key by a certifying authority through publication of a certificate on a certificate revocation list (CRL) as follows:

Whenever any user, entity or device “verifies” a digitally signed “certificate,” whether a manufacturer’s certificate or an escrow certificate, issued by a certifying authority or manufacturer, it is common practice in most or all actual and proposed public key certificate management systems (and it is assumed throughout this disclosure) that the user, entity or device also checks any applicable “certificate revocation list” (“CRL”) in order to determine whether the certifying authority or other issuer has distributed, propagated or otherwise made available a list of revoked certificates that is updated in accord with an appropriate security policy and whether, based upon the issuer name and certificate number, the certificate has been revoked. A certificate issued to a user

The combination of *Doonan* and *Sudia* urged by the Examiner thus discloses the revocation of the message recipient’s public key by publication on a certificate revocation list (CRL) of the message recipient’s certificate.

However, *Doonan* and *Sudia's* disclosure of conventional revocation of a recipient’s public key through CRL publication does not teach or suggest “thereafter, preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system”, as recited in Claim 1. As described by *Sudia* at col. 22, line 51 *et seq.*, key

revocation through conventional CRL publication relies upon a message recipient checking a CRL to verify a digitally signed certificate, where the presence of a certificate in the CRL indicates that the certificate has been revoked and its absence from the CRL signifies the certificate's validity. Such revocation can be said to be made "at" the certifying authority that publishes the CRL or perhaps even "at" the recipient system that receives the message from the encrypting data processing system and performs the validation. However, the conventional publication of the recipient's public key on a CRL as taught by *Doonan* and *Sudia* does not revoke the public key "at" the encrypting data processing system in that the encrypting data processing system (i.e., the sending system) in the system of *Doonan* and *Sudia* can still generate messages signed with a recipient's public key for which the certificate is published on a CRL. Moreover, the encrypting data processing system in the conventional CRL publication scheme disclosed by *Doonan* and *Sudia* does not (and need not) check the CRL prior to generating, signing and transmitting an encrypted message. Consequently, the combination of *Doonan* and *Sudia* does not disclose revoking the associated key at the encrypting data processing system as claimed.

The revocation of the associated key at the encrypting data processing system as recited in exemplary Claim 1 has a number of advantages over the conventional revocation through publication on a CRL as disclosed by *Doonan* and *Sudia*. In particular, by revoking the associated key at the encrypting data processing system, the recipient need not check a CRL to verify the association of the sender with the encrypted message and is not subject to the time-granularity problem (described, for example, at page 4, lines 8-32) by which publication of the certificate on the CRL may be subject to delay.

In view of the failure of the combination of *Doonan* and *Sudia* to disclose each feature recited in exemplary Claim 1, and in particular, the claimed use and revocation of an associated key at an encrypting data processing system, Appellants respectfully submit that Claim 1, similar Claims 9 and 17 and their respective dependent claims are not rendered unpatentable under 35 U.S.C. § 103.

II. The combination of *Doonan* and *Sudia* does not disclose each feature of exemplary Claim 7

The rejection of exemplary Claim 7 in view of *Doonan* and *Sudia* is also not well founded and should be reversed because the combination of cited references does not disclose “communicating an encrypted associated key to validate the association of the user with the encrypted messages,” as claimed. That is, the combination of cited references does not disclose the communication of both an encrypted associated key and an encrypted user key.

With reference to the above feature of Claim 7, page 8 of the Final Office Action again cites col. 5, lines 63-67 of *Doonan*, which as noted above discloses:

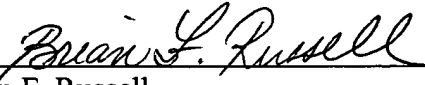
The composite message P is first encrypted to form encrypted message Pe, using a randomly-generated symmetric encryption key Ks. The symmetric key Ks is then itself encrypted using the public key published in a digital certificate owned by the recipient, to form [the encrypted symmetric key] Kp. The sender then constructs a transmittal message Pt that comprises the encrypted message Pe and the encrypted symmetric key Kp.

That is, *Doonan* discloses the communication of only the encrypted symmetric key Kp relied upon by the Examiner as teaching the claimed “encrypted user key.” The Examiner does not cite any portion of *Doonan* or *Sudia* as disclosing the claimed “encrypted associated key” or its communication to “validate the association of the user with the encrypted messages,” as claimed. Consequently, the Examiner has failed to establish a *prima facie* case of obviousness with respect to Claim 7 and similar Claims 15 and 23.

III. Conclusion

The foregoing remarks demonstrate that the combination of cited references does not teach or suggest each feature of Claims 1-24 as required to support a rejection under 35 U.S.C. § 103. Appellants therefore respectfully request the Board to reverse the final rejection of each of Claims 1-24.

Respectfully submitted,



Brian F. Russell
Reg. No. 40,796
DILLON & YUDELL LLP
8911 N. Capital of Texas Highway
Suite 2110
Austin, Texas 78759
(512) 343-6116
ATTORNEY FOR APPELLANTS

APPENDIX A
CURRENTLY PENDING CLAIMS

1. A method for managing a user key used to sign a message for a data processing system, said method comprising:

assigning a user key to a user and storing the user key in an encrypting data processing system utilized to encrypt messages;

encrypting the messages with the user key;

storing an associated key in the encrypting data processing system and encrypting the user key with the associated key to obtain an encrypted user key;

said encrypting data processing system communicating at least one encrypted message together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system; and

thereafter, preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system.

2. The method according to Claim 1, further comprising:

decrypting the user key with the associated key; and

decrypting the messages with the user key.

3. The method according to Claim 1, wherein:

the encrypting data processing system further comprises a client system and a server system coupled for communication, said client system having a client memory device and said server system having an encryption chip and a server memory device;

storing the user key further comprises storing the user key in the client memory device;

storing the associated key further comprises storing the associated key in the server memory device; and

preventing validation further comprises preventing validation of messages associated with the user by eliminating the associated key from the server memory device.

4. The method according to Claim 3, wherein encrypting the messages further comprises:

sending the messages to be encrypted from the client system to the server system;
encrypting the messages using the encryption chip of the server system; and
sending the encrypted messages from the server system to the client system.

5. The method according to Claim 4, further comprising:
erasing from the server system all data relating to the encrypted messages after the encrypted messages are sent from the server system to the client system.
6. The method according to Claim 1, further comprising:
encrypting the associated key by using an encryption chip key which is stored on an encryption chip of the encrypting data processing system.
7. The method according to Claim 6, further comprising:
communicating an encrypted associated key to validate the association of the user with the encrypted messages.
8. The method according to Claim 7, further comprising:
decrypting the associated key with the encryption chip key.
9. A system for managing a user key used to sign a message, said system comprising:
means for assigning a user key to a user;
means for storing the user key;
means for encrypting the messages with the user key;
means for storing an associated key;
means for encrypting the user key with the associated key to obtain an encrypted user key;
means for communicating at least one encrypted message together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system; and
means for thereafter preventing validation of the association of the user with messages by revoking the associated key in said system.

10. The system according to Claim 9, further comprising:
means for decrypting the user key with the associated key; and
means for decrypting the messages with the user key.
11. The system according to Claim 9, wherein:
the system further comprises a client system and a server system coupled together for communication, said client system having a client memory device and said server system having an encryption chip and a server memory device;
said means for storing the user key further comprises means for storing the user key in the client memory device;
said means for storing the associated key further comprises means for storing the associated key in the server memory device; and
said means for preventing validation further comprises means for preventing the validation of messages associated with the user by eliminating the associated key from the server memory device.
12. The system according to Claim 11, wherein said means for encrypting the messages further comprises:
means for sending the messages to be encrypted from the client system to the server system;
means for encrypting the messages using the encryption chip of the server system; and
means for sending the encrypted messages from the server system to the client system.
13. The system according to Claim 12, further comprising:
means for erasing from the server system all data relating to the encrypted messages after the encrypted messages are sent from the server system to the client system.
14. The system according to Claim 9, further comprising:
an encryption chip that encrypts the associated key by using an encryption chip key stored within the encryption chip .

15. The system according to Claim 14, further comprising:
means for communicating an encrypted associated key to validate the association of the user with the encrypted messages.
16. The system according to Claim 15, further comprising:
means for decrypting the associated key with the encryption chip key.
17. A program product for managing a user key used to sign a message, said program product comprising:
a control program including:
instruction means for assigning a user key to a user and for storing the user key in an encrypting data processing system utilized to encrypt messages;
instruction means for encrypting the messages with the user key;
instruction means for storing an associated key in the encrypting data processing system and for encrypting the user key with the associated key to obtain an encrypted user key;
instruction means for communicating at least one encrypted message together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system;
instruction means for thereafter preventing validation of the association of the user with messages by revoking the associated key within the encrypting data processing system; and
computer usable media bearing said control program.
18. The program product according to Claim 17, further comprising:
instruction means for decrypting the user key with the associated key; and
instruction means for decrypting the messages with the user key.
19. The program product according to Claim 17, wherein:

the encrypting data processing system further comprises a client system and a server system coupled together for communication, said client system having a client memory device and said server system having an encryption chip and a server memory device;

said instruction means for storing the user key further comprises instruction means for storing the user key in the client memory device;

said instruction means for storing the associated key further comprises instruction means for storing the associated key in the server memory device; and

said instruction means for preventing validation further comprises instruction means for preventing the validation of the messages associated with the user by eliminating the associated key from the server memory device.

20. The program product according to Claim 19, wherein said instruction means for encrypting the messages further comprises:

instruction means for sending the messages to be encrypted from the client system to the server system;

instruction means for encrypting the messages using the encryption chip of the server system; and

instruction means for sending the encrypted messages from the server system to the client system.

21. The program product according to Claim 20, further comprising:

instruction means for erasing from the server system all data relating to the encrypted messages after the encrypted messages are sent from the server system to the client system.

22. The program product according to Claim 17, further comprising:

instruction means for encrypting the associated key by using an encryption chip key which is stored on an encryption chip of the data processing system.

23. The program product according to Claim 22, further comprising:

instruction means for communicating an encrypted associated key to validate the association of the user with the encrypted messages.

24. The program product according to Claim 23, further comprising:
instruction means for decrypting the associated key with the encryption chip key.

APPENDIX B
EVIDENCE APPENDIX

(none)

APPENDIX C
RELATED PROCEEDINGS APPENDIX

(none)